Christopher L. Springer (SBN 291180)
KELLER ROHRBACK L.L.P.
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Telephone: (805) 456-1496
Facsimile: (805) 456-1497
cspringer@kellerrohrback.com

Attorney for Plaintiff Star Ghanaat

Additional counsel listed on signature page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

Star Ghanaat, individually and on behalf of all others similarly situated, Plaintiff, v. AT&T, Inc., Defendant.	No. **COMPLAINT** **CLASS ACTION** **JURY TRIAL DEMANDED**

1. Plaintiff Star Ghanaat brings this action against Defendant AT&T, Inc. ("Defendant" or "AT&T") on behalf of the victims of a targeted cyberattack on AT&T that was announced on July 12, 2024 ("the Data Breach"). Plaintiff brings this action against Defendant for its failure to properly secure and safeguard the sensitive personal information of herself and all those similarly situated, and, in compensation for that failure, she seeks monetary damages, restitution, and/or injunctive relief. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only AT&T (as well as the cybercriminals who perpetrated the Data Breach) have knowledge of what information was compromised, Plaintiff reserves the right to supplement these allegations with additional facts and injuries as they are discovered.

I. JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists, as Defendant is a citizen of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

3. This Court has personal jurisdiction over Defendant because AT&T is authorized to and regularly conducts business in the State of California, including by selling, marketing, and advertising its products and services to consumers located in the State of California and within this District. Defendant therefore has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

4. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

II. PARTIES

5. Plaintiff Star Ghanaat is a resident of Concord, California, whose wireless carrier, for the period May 1, 2022 to October 31, 2022 and on January 2, 2023, was Xfinity Mobile. From May through October 2022, she frequently called and texted with AT&T Mobile customers. On January 2, 2023, on information and belief, she called and texted with at least one AT&T Mobile customer.

6. Defendant AT&T, Inc. is a corporation organized under the state laws of Delaware with its principal place of business located in Dallas, Texas. It is one of the largest wireless carriers in the country.

III. FACTUAL ALLEGATIONS

7. As a wireless carrier, Defendant collected a variety of information about Plaintiff and Class Members, including some personally identifiable information ("PII"), such as names, phone numbers, cell site identification numbers, and other sensitive information, when Plaintiff and Class Members communicated with AT&T Mobile customers.

8. In the course of collecting personally identifying information from consumers,

including Plaintiff, Defendant had an obligation to provide confidentiality and adequate security for the data it collected. Defendant also represented and promised its customers that it provides such confidentiality and security through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

9. For instance, Defendant's Privacy Notice provides:

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[1]

10. Defendant also provides on its website that:

> As the digital landscape grows, our employees, customers and partners depend on us to help protect them from cyberattacks. AT&T operates one of the world's most advanced and powerful global backbone networks and is a recognized leading provider of IP-based communication services. We have a responsibility to safeguard customer information. Security is at the core of our network and central to everything we do.
>
> We regularly evaluate and deploy new tools and systems that deliver highly effective safeguards against attempted cyberattacks. We also invest in customer solutions and trainings to raise awareness of customers' agency in protecting themselves from fraud.[2]

11. Defendant further provides on its website that:

> AT&T uses a consistent, disciplined global process to promptly identify security incidents and threats, minimize the loss or compromise of information, and facilitate incident resolution. AT&T maintains 24/7, near-real-time security monitoring of the AT&T network for investigation, action and response to network security events. Our threat management platform and program provide near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trending analysis and predictive security alerting. AT&T uses the same set of security tools to manage our global network that we use for enterprise customers.[3]

12. AT&T customers relied on these promises and on this sophisticated business entity to

[1] AT&T, Inc., *AT&T Privacy Notice* (July 17, 2024), https://about.att.com/privacy/privacy-notice.html.
[2] AT&T, Inc., *Network & Data Security*, https://sustainability.att.com/priority-topics/network-data-security (last visited July 18, 2024).
[3] *Id.*

keep their sensitive personally identifiable information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers of other wireless carriers, including Plaintiff and Class Members, also relied on AT&T to keep their sensitive personally identifiable information that AT&T received when they communicated with AT&T wireless customers confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their personally identifiable information.

A. The Data Breach

13. In April 2024, AT&T became aware that a third party or third parties accessed and captured the call logs of more than 100 million AT&T wireless customers. The call log information contains the records of calls and text messages from the six months between May 1, 2022 and October 31, 2022, as well as on January 2, 2023. Because the information identifies each telephone number that an AT&T cellular number interacted with during the time period, it also includes the records of consumers who receive their phone service from carriers other than AT&T, including, upon information and belief, Plaintiff and Class Members.

14. This information, the "Call Log Information," comprises an array of highly personal information for each customer, including the phone number of the AT&T customer, the phone numbers that the AT&T customer called or texted, the number of times the AT&T customer interacted with each phone number, and call durations ("Personal Information"). Many records also included information about the wireless customers' locations, in the form of cell site ID numbers.

15. AT&T had uploaded the Call Log Information to the servers of a third party called Snowflake, a company that provides cloud-storage services, effectively outsourcing its responsibility to safeguard the consumer information that was ultimately stolen by hackers.

16. Shockingly, AT&T's account on Snowflake could be accessed simply through a username and password. Multi-factor authentication was not required.

17. Even more shockingly, ***Snowflake made multi-factor authentication available to its corporate customers—AT&T just decided not to use it.***

18. As a result of AT&T's failure to adequately safeguard the Call Log Information,

cybercriminals accessed AT&T's Call Log information through Snowflake.

19. The Data Breach here was not the only recent theft of personally identifiable information stored on Snowflake. Other companies, including Ticketmaster, QuoteWizard, Santander, LendingTree, and Advance Auto Parts, have recently confirmed that they had customer data stolen from Snowflake.

B. AT&T's failure to responsibly protect consumers' personally identifiable information

20. The Data Breach is attributable to AT&T's failure to comply with state and federal laws and requirements as well as industry standards governing the protection of personally identifiable information.

21. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license, or maintain personally identifiable information to implement and maintain "reasonable security procedures and practices" and to protect personally identifiable information from unauthorized access. California is one such state, which requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b).

22. AT&T also failed to comply with Federal Trade Commission ("FTC") guidance on protecting personally identifiable information and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, a failure by a company like Defendant to use reasonable measures to protect personally identifiable information. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive consumer data should factor into virtually all business decisions.

23. The FTC recommends, among other things:

a. limiting access to consumer information to those who have a legitimate business need for it;

b. encrypting consumer information on system and in transit;

c. implementing multi-factor authentication for anyone accessing consumer information;

d. implementing procedures and controls to monitor when authorized users are accessing consumer information;

e. maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to consumer information; and

f. implementing procedures and controls to detect unauthorized access to consumer information, including monitoring activity logs for signs of unauthorized access to consumer information.

24. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices.

25. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[4] The guidelines note businesses should protect the personal consumer information that they keep; properly dispose of personally identifiable information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion-detection system to identify a breach as soon as it occurs; monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

26. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive consumer information; require strong passwords be used by employees with access to sensitive consumer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

27. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate

[4] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

28. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

29. AT&T was aware of its obligations to protect consumers' personally identifiable information and privacy before and during the Data Breach yet failed to take reasonable steps to protect consumers' information from unauthorized access. It was also aware of the significant repercussions that could result if it failed to do so, because AT&T collected personally identifiable information from millions of consumers and it knew that this PII, if hacked, would result in injury to consumers, including Plaintiff and Class Members. In fact, AT&T should have been particularly aware of its obligations and the potential repercussions of not fulfilling those obligations as it had suffered a recent massive data breach in March 2024 involving the PII of 73 million of AT&T's current and former customers.

C. Injuries to Plaintiff and Class Members

30. The personally identifiable information of consumers that has now been stolen, even without the content of calls and texts, enables third parties to identify individual persons and uncover otherwise private (and extremely sensitive) information about them. Moreover, as AT&T itself acknowledged in response to the Data Breach, "there are often ways, using publicly available online tools, to find the name associated with a specific telephone number."[5]

31. Consider a 2016 study authored by computer scientists from Stanford University.[6] These scientists, using telephone metadata of the kind that was accessed in the Data Breach, were able to learn a concerning amount of highly sensitive information about the telephone users. Through manual and automated searches on the internet, they identified 82% of the users' names. They also were able to uncover the names of businesses users had called; when plotted on a map, they typically

[5] AT&T, *AT&T Addresses Illegal Download of Customer Data* (July 12, 2024), https://about.att.com/story/2024/addressing-illegal-download.html.

[6] Jonathan Meyer et al., *Evaluating the Privacy Properties of Telephone Metadata*, PNAS (May 16, 2016), https://www.pnas.org/doi/full/10.1073/pnas.1508081113.

clustered so as to reveal where the telephone user likely lived. Indeed, the scientists were nearly 90% accurate in placing users within 50 miles of their home. Note, too, that these statistics almost certainly understate the extent to which telephone metadata can reveal names and locations, since the scientists used free public databases available on the internet, rather than commercial databases that condition access on payment or datasets available to cybercriminals on the dark web.

32. In this same study, the authors discussed how they were able to infer extremely sensitive information about the telephone users. The metadata allowed the scientists to infer that one person had a serious heart condition, that another owned a rifle, that another had multiple sclerosis, and that still another had just become pregnant.

33. Knowledge of a person's physical location, contact habits, and telephone number also enables a wide range of fraud and other harm. For example, once a fraudster figures out that a telephone user banks at Wells Fargo, it is easier to pose as Wells Fargo in a fraudulent telephone call or text. This is just one example, however, and the potential permutations of such attempts at fraud are endless. Under any permutation, however, those whose Personal Information has been accessed in the Data Breach are harmed: a malicious actor credibly poses as a trusted third party, the individual discloses further sensitive information to the malicious actor, and the malicious actor uses that information to commit identity theft, fraud, or other cybercrimes.

34. Further, malicious actors often wait months or years to use the information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen information, meaning individuals can be the victim of several instances of identity theft, fraud, or other cybercrimes stemming from a single data breach.

35. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." Moreover, there is often significant lag time between when a person suffers harm due to theft of their personally identifiable information and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor her accounts for years to ensure her personally identifiable

information obtained in the Data Breach is not used to harm her. Plaintiff and the Class have been harmed by the value of identity protection services and/or mitigation measures they must purchase in the future to ameliorate the heightened and imminent risk of identity theft, fraud, and other cybercrimes due to the Data Breach.

36. Reporting on the Data Breach provides additional details. According to an article in Wired, which is based on communications with the security researcher who disclosed the breach to AT&T and was in contact with the hacker, the hacker who accessed the AT&T data "demonstrated how easily he could identify the owners of the numbers using a reverse-lookup program that identified by name the family members, colleagues, and others attached to the phone numbers who communicated with them."[7]

37. Even if the hacker has deleted the data, it is unclear how many people may have received or otherwise accessed the data between the time the hacker stole it and when he might have deleted it.[8] Likewise, there is no way to determine whether anyone who received or accessed the data before it was taken down has made it available to or otherwise disseminated it to others, and no way to track down and confirm the deletion of any such information.

38. Thus, the risk of these harms is ongoing, and Plaintiff and Class Members continue to be at imminent risk of suffering future damages associated with the unauthorized use and misuse of their information, as there is an ongoing risk that data thieves and malicious actors who accessed the stolen information will use the stolen information to the detriment of Plaintiff and Class Members for many years to come.

39. As a direct result of the Data Breach, Plaintiff and Class Members have suffered actual and/or attempted identity theft and fraud, and they will continue to be exposed to a heightened and imminent risk of identity theft and fraud, potentially for the rest of their lives. Plaintiff and Class Members must now and in the future closely monitor their medical, insurance, and financial accounts to guard against identity theft and fraud.

40. For this reason, Class Members may incur out-of-pocket costs for purchasing protective

[7] Kim Zetter, *AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records*, Wired (July 14, 2024), https://www.wired.com/story/atandt-paid-hacker-300000-to-delete-stolen-call-records/.

[8] *Id.*

measures to deter and detect identity theft and fraud, for purchasing protective measures to mitigate against the misuse of their information, and for taking efforts to mitigate the harms once identity theft and/or fraud is discovered.

41. As a direct and proximate result of the Data Breach and subsequent exposure of their personally identifiable information, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid the misuse of their information, protect against potential unauthorized and fraudulent charges, and deal with spam phone calls, letters, text messages, and emails received as a result of the Data Breach and the unauthorized disclosure and misuse of their personally identifiable information.

42. Plaintiff and Class Members have also realized harm in the lost or reduced value of their personally identifiable information. Plaintiff's personally identifiable information is not only valuable to AT&T, but Plaintiff also places high value on her personally identifiable information based on her understanding that it is a financial asset to companies that collect it.

43. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the cybercriminal's access to Plaintiff's information that was permitted without authorization. This market value can be determined by reference to both legitimate and illegitimate markets for personally identifiable information.

44. Moreover, Plaintiff and Class Members value the privacy of this information and expect companies that obtain and maintain their PII to allocate enough resources to ensure it is adequately protected.

45. As a wireless carrier, AT&T had an obligation to implement reasonable security measures to protect the personally identifiable information of Plaintiff and Class Members.

46. Given AT&T's failure to protect Plaintiff's and the Class Members' personally identifiable information, Plaintiff has a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects her from suffering further harm, as her personally identifiable information remains in AT&T's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on a large class of persons.

47. In sum, Plaintiff and Class Members were injured by the following: (i) theft of their personally identifiable information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their personally identifiable information; (iii) loss of value of their personally identifiable information; (iv) the lost value of access to Plaintiff's and Class Members' personally identifiable information permitted by AT&T; (v) the amount of the actuarial present value of high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; (vi) AT&T's retention of profits attributable to Plaintiff's and Class Members' personally identifiable information that AT&T failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; and (ix) nominal damages.

IV. CLASS ACTION ALLEGATIONS

A. Nationwide class

48. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States who are not customers of AT&T and whose personally identifiable information was exfiltrated in the Data Breach.

49. The Nationwide Class asserts claims against AT&T for negligence (Count 1), negligence per se (Count 2), and declaratory judgment (Count 3).

B. California subclass

50. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of a California Subclass in the alternative to the nationwide claims (Counts 1 through 3), as well as with respect to statutory claims under the California Consumer Privacy Act, Cal. Civ. Code § 1798, et seq. (Count 4), the California Customer Records Act, Cal. Civ. Code § 1798.80, et seq. (Count 5), and Invasion of Privacy, Cal. Const. Art. 1 § 1 (Count 6), on behalf of a California Subclass, defined as follows:

> All natural persons residing in California who are not customers of AT&T and whose personally identifiable information was exfiltrated in the Data Breach.

51. Excluded from the Nationwide Class and the California Subclass (collectively, the "Class") are AT&T, any entity in which AT&T has a controlling interest, and AT&T's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

52. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Nationwide Class and the California Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, AT&T has acknowledged that millions of individuals' personally identifiable information has been compromised. On information and belief, information about members of the Nationwide Class and the California Subclass, who are not AT&T customers, is available from AT&T's records, including through information compromised in the Data Breach, and those Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of individuals in the Nationwide Class and at least thousands of individuals in the California Subclass, making joinder of all Class Members impracticable.

53. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** As to both the Nationwide Class and the California Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. The common questions include:

a. Whether AT&T had a duty to protect the personally identifiable information of consumers who use other wireless carriers;

b. Whether AT&T failed to take reasonable and prudent security measures to ensure the personally identifiable information of consumers that it collects and maintains was protected;

c. Whether AT&T failed to take available steps to prevent and stop the Data Breach from happening;

d. Whether AT&T knew or should have known that the personally identifiable information

it maintains on customers who use other wireless carriers was vulnerable to compromise;

e. Whether AT&T was negligent in failing to implement reasonable and adequate security procedures and practices;

f. Whether AT&T's security measures to protect the personally identifiable information it maintains about other carriers' customers were reasonable in light known legal requirements;

g. Whether AT&T's conduct constituted unfair or deceptive trade practices;

h. Whether AT&T violated state or federal law when it failed to implement reasonable security procedures and practices;

i. Which security procedures and notification procedures AT&T should be required to implement;

j. Whether AT&T had any contractual obligations or other duties to provide for the security of personally identifiable information of individuals who are not its customers, but who communicate with its customers;

k. What security measures, if any, must be implemented by AT&T to comply with its contractual obligations or other duties;

l. Whether AT&T violated state consumer protection laws in connection with the actions described herein;

m. Whether AT&T failed to notify Plaintiff and Class Members as soon as practicable and without delay after the Data Breach was discovered;

n. Whether AT&T's conduct resulted in or was the proximate cause of the loss of the personally identifiable information of Plaintiff and Class Members;

o. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of AT&T's failure to reasonably protect their personally identifiable information;

p. Whether and how AT&T should retain Plaintiff's and Class Members' valuable personally identifiable information; and,

q. Whether Plaintiff and Class Members are entitled to damages or injunctive relief.

54. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Nationwide Class and the California Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiff's personally identifiable information was in AT&T's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members, and Plaintiff seeks relief consistent with the relief of the Class.

55. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Nationwide Class and the California Subclass because Plaintiff is a member of the Nationwide Class and the California Subclass and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

56. **Predominance and Superiority: Federal Rule of Civil Procedure 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against AT&T, and thus individual litigation to redress AT&T's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale,

and comprehensive supervision by a single court.

57. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for AT&T or would be dispositive of the interests of members of the proposed Class.

58. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Rule 23(b)(2) and (c). AT&T, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

59. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

V. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT ONE — NEGLIGENCE
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the California Subclass

60. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

61. In the course of communicating with AT&T customers, Plaintiff and Class Members were required to provide their sensitive Personal Information to AT&T.

62. AT&T owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting their Personal Information in AT&T's possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing AT&T's security systems to ensure that Plaintiff's and Class Members' Personal Information in AT&T's possession was adequately secured and protected; (b) implementing processes to ensure that any third parties to which AT&T disclosed Plaintiff's and Class Members' Personal Information implemented, maintain, and tested security systems to ensure that the information was adequately secured and

protected; (c) implementing and utilizing processes to ensure that the transfer of Plaintiff's and Class Members' Personal Information between AT&T and third parties was secured and protected; (d) implementing processes that would detect unauthorized access to the Personal Information AT&T maintains in a timely manner; (e) timely acting upon warnings and alerts, including those generated by AT&T's own security systems, regarding unauthorized access to the Personal Information it maintains; and (f) maintaining data security measures consistent with industry standards.

63. AT&T duty to use reasonable care arose from several sources, including but not limited to those described herein.

64. AT&T had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by AT&T's failure to protect their Personal Information because cybercriminals routinely attempt to steal such information and use it for nefarious purposes, AT&T knew that it was more likely than not Plaintiff and other Class Members would be harmed if AT&T allowed such a breach.

65. AT&T's duty to use reasonable security measures also arose as a result of the special relationship that existed between AT&T, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members could not opt out of providing AT&T with sensitive Personal Information when they communicated with AT&T customers. AT&T alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

66. AT&T's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as AT&T. Various FTC publications and data security breach orders further form the basis of AT&T's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

67. AT&T's duty also arose from its superior position to protect against the harm suffered

by Plaintiff and Class Members as a result of the Data Breach.

68. AT&T admits that it has a responsibility to protect the Personal Information with which it is entrusted.

69. AT&T knew or should have known that its data storage architecture was vulnerable to unauthorized access and targeting by cybercriminals for the purpose of stealing and misusing confidential Personal Information.

70. AT&T also had a duty to safeguard the Personal Information of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require AT&T to reasonably safeguard sensitive Personal Information, as detailed herein.

71. Timely, adequate notification was required, appropriate, and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid or mitigate identity theft or fraud, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by AT&T's misconduct.

72. AT&T breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. AT&T breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Personal Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff's and the Class Members' Personal Information in AT&T's possession had been or was reasonably believed to have been stolen or compromised.

73. But for AT&T's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

74. AT&T's failure to take proper security measures to protect the sensitive Personal Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional

act, namely the unauthorized access of Plaintiff's and Class Members' Personal Information.

75. Plaintiff and Class Members were foreseeable victims of AT&T's inadequate data security practices, and it was also foreseeable that AT&T's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

76. As a direct and proximate result of AT&T's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, and impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; nominal and general damages and other economic and non-economic harm.

COUNT TWO — NEGLIGENCE *PER SE*
On Behalf of Plaintiff and the Nationwide Class,
or Alternatively, on Behalf of Plaintiff and the California Subclass

77. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

78. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as AT&T of failing to use reasonable measures to protect Personal Information.

79. The FTC publications and orders also form the basis of AT&T's duty.

80. AT&T violated Section 5 of the FTC Act by failing to use reasonable measures to

protect Personal Information and not complying with applicable industry standards. AT&T's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, the foreseeable consequences of a data breach involving the highly sensitive Personal Information it maintains, including specifically the damages that would result to Plaintiff and Class Members, and the obviousness of its failure to comply with applicable industry standards such as dual-factor authentication.

81. In addition, under state data security statutes, AT&T had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Personal Information.

82. AT&T's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

83. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

84. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

85. AT&T breached its duties to Plaintiff and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiff's and Class Members' Personal Information.

86. Plaintiff and Class Members were foreseeable victims of AT&T's violations of the FTC Act and state data security statutes. AT&T knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' Personal Information would cause damage to Plaintiff and Class Members.

87. But for AT&T's violation of the applicable laws and regulations, Plaintiff's and Class Members' Personal Information would not have been accessed by unauthorized parties.

88. As a direct and proximate result of AT&T's negligence per se, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such

injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT THREE — DECLARATORY JUDGMENT
On Behalf of Plaintiff and the Nationwide Class,
or Alternatively, on Behalf of Plaintiff and the California Subclass

89. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

90. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

91. An actual controversy has arisen in the wake of the AT&T Data Breach regarding AT&T's present and prospective common law and other duties to reasonably safeguard consumers' Personal Information and whether AT&T is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Personal Information. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future given the publicity around the Data Breach and the nature and

quantity of the Personal Information stored by AT&T.

92. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. AT&T continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. AT&T continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

93. The Court also should issue corresponding prospective injunctive relief requiring AT&T to employ adequate security protocols consistent with the law and industry standards to protect consumers' Personal Information.

94. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at AT&T. The risk of another such breach is real, immediate, and substantial. If another breach at AT&T occurs, Plaintiff and Class Members will not have an adequate remedy at law.

95. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to AT&T if an injunction is issued. Among other things, if another significant data breach occurs at AT&T, Plaintiff and Class Members will likely be subjected to substantial identity theft and other harms. On the other hand, the cost to AT&T of complying with an injunction by employing reasonable prospective data security measures is relatively limited, and AT&T has a pre-existing legal obligation to employ such measures.

96. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AT&T, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and the millions of consumers whose confidential information would be further compromised.

VI. CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT FOUR — CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798, *ET SEQ.*

97. Plaintiff, individually and on behalf of the California Subclass, incorporates all

foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach.

98. The California Consumer Privacy Act ("CCPA"), portions of which were operative beginning January 1, 2020, was enacted by the California Legislature "to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80)." Cal. Civ. Code § 1798.175. The CCPA applies to "the collection and sale of all personal information collected by a business from consumers." *Id.*

99. "Businesses," defined to include a "corporation" that "collects consumers' personal information" that "does business in the State of California" and has annual gross revenues in excess of $25 million, are required to comply with the CCPA. Cal. Civ. Code §1798.140(d). AT&T is a "business" under the CCPA.

100. The CCPA protects "consumers." "Consumer" is defined as "a natural person who is a California resident[.]" Cal. Civ. Code § 1798.140(i). Plaintiff and the California Subclass are "consumers" within the meaning of the CCPA.

101. The protections of the CCPA extend to "personal information" of consumers. "Personal information" is defined by the CCPA to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1). "Personal information includes" information that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1)(A). The Private Information of Plaintiff and the California Subclass that was compromised in the Data Breach included "personal information" within the meaning of the CCPA.

102. The CCPA provides consumers with the right to institute a civil action where the consumers' "nonencrypted and nonredacted personal information" was the subject of "an unauthorized

access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information[.]" Cal. Civ. Code § 1798.150(a)(1).

103. Plaintiff's and the California Subclass's nonencrypted and nonredacted personal information as defined in § 1798.81.5 in the form of their Private Information was collected by AT&T.

104. AT&T, as a "business" covered by the CCPA, owed a duty to Plaintiff and the California Subclass to implement and maintain reasonable security procedures and practices to protect the Private Information of Plaintiff and the California Subclass.

105. AT&T breached this duty. One or more third parties accessed Plaintiff's and the California Subclass's Private Information, including but not limited to phone numbers and geolocation data that are reasonably capable of being associated with particular consumers. The fact that Plaintiff's and the California Subclass's Private Information was accessed without authorization establishes that AT&T did not take adequate data security measures to store and protect wireless customers' Private Information. AT&T failed to take adequate security measures to protect Plaintiff's and the California Subclass's Private Information.

106. As a direct and proximate result of AT&T's acts and omissions, Plaintiff and the California Subclass were subjected to unauthorized access and exfiltration, theft, or disclosure as a result of AT&T's violation of the duty.

107. On behalf of the California Subclass, Plaintiff seeks injunctive relief in the form of an order (a) enjoining AT&T from continuing to violate the CCPA; and (b) requiring AT&T to employ adequate security practices consistent with law and industry standards to protect California Subclass members' Private Information.

108. Plaintiff and the California Subclass are at high risk of suffering, or have already suffered, injuries that cannot be remedied monetarily, such as reductions to their credit scores and identity theft. As such, the remedies at law available to Plaintiff and the California Subclass are wholly inadequate by themselves.

109. The full extent of the existing and potential harm caused by AT&T's failure to protect the Private Information of wireless users who contacted AT&T customers cannot be remedied by

monetary damages alone because monetary compensation does nothing to prevent the reoccurrence of another data breach in the future.

110. Plaintiff and the California Subclass seek injunctive relief, actual pecuniary damages suffered as a result of AT&T's violations described herein, and any other relief the Court deems proper pursuant to this section, such as attorneys' fees.

111. On August 12, 2024, Plaintiff Star Ghanaat sent written notice identifying AT&T's violation of Cal. Civ. Code § 1798.150(a) and demanding that the Data Breach be cured. Accordingly, Plaintiff seeks all relief available under the CCPA, including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT FIVE — CALIFORNIA CUSTOMER RECORDS ACT, CAL. CIV. CODE § 1798.80, *ET SEQ.*

112. Plaintiff, individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach.

113. The California Customer Records Act requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5.

114. AT&T is subject to the California Customer Records Act because it owns, maintains, and licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and the California Subclass.

115. AT&T violated Cal. Civ. Code § 1798.81.5 by failing to adopt and utilize reasonable measures to protect Plaintiff's personal information.

116. As a direct and proximate result of AT&T's violations of Cal. Civ. Code § 1798.81.5, the Data Breach described above occurred.

117. Plaintiff suffered damages and injury including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of her personally identifying information.

118. Plaintiff seeks relief under Cal. Civ. Code § 1798.84 including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

COUNT SIX — INVASION OF PRIVACY, CAL. CONST. ART. 1 § 1

119. Plaintiff, individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach.

120. California established the right to privacy in Article I, Section 1 of the California Constitution.

121. Plaintiff and the California Subclass had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

122. AT&T owed a duty to all individuals who communicated with AT&T wireless customers, including Plaintiff and the California Subclass, to keep their Private Information contained as a part thereof, confidential.

123. AT&T failed to protect and released to unknown and unauthorized third parties the Private Information of Plaintiff and the California Subclass.

124. AT&T allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiff and the California Subclass, by way of AT&T's failure to protect the Private Information.

125. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the California Subclass is highly offensive to a reasonable person.

126. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the California Subclass were required to disclose their Private Information to AT&T as

part of communicating with users of AT&T's cellular service, but with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the California Subclass were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

127. The Data Breach at the hands of AT&T constitutes an intentional interference with Plaintiff's and the California Subclass's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

128. AT&T acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

129. Because AT&T acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the California Subclass.

130. As a proximate result of the above acts and omissions of AT&T, the Private Information of Plaintiff and the California Subclass was disclosed to third parties without authorization, causing Plaintiff and the California Subclass to suffer damages.

131. Unless and until enjoined, and restrained by order of this Court, AT&T's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the California Subclass in that the Private Information compromised in the Data Breach can be viewed, distributed, and used by unauthorized persons for years to come.

132. Plaintiff, on behalf of the California Subclass, seeks injunctive relief requiring AT&T to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) to provide adequate identity theft monitoring and other threat reduction measures as needed to all members of the California Subclass.

133. Plaintiff and the California Subclass have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the California Subclass.

VII. REQUEST FOR RELIEF

Plaintiff, individually and on behalf of members of the Nationwide Class and California Subclass, as applicable, respectfully requests that the Court enter judgment in Plaintiff's favor and against AT&T, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit AT&T from continuing to engage in the unlawful acts, omissions, and practices described herein, including;

a. Prohibiting AT&T from engaging in the wrongful and unlawful acts described herein;

b. Requiring AT&T to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring AT&T to delete, destroy and purge the Personal Information of Plaintiff and Class Members unless AT&T can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. Requiring AT&T to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Personal Information;

e. Requiring AT&T to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on AT&T's systems on a periodic basis, and ordering AT&T to promptly correct any problems or issues detected by such third-party security auditors;

f. Requiring AT&T to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring AT&T to audit, test, and train its security personnel regarding any new or modified procedures;

h. Requiring AT&T to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling Personal Information, as well as protecting the Personal Information of Plaintiff and Class Members;

i. Requiring AT&T to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

j. Requiring AT&T to implement a system of testing to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with AT&T's policies, programs and systems for protecting Personal Information;

k. Requiring AT&T to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor AT&T's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l. Requiring AT&T to meaningfully educate all Class Members about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps affected individuals must take to protect themselves;

m. Requiring AT&T to implement logging and monitoring programs sufficient to track traffic to and from AT&T servers; and

n. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis AT&T's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

3. That the Court award Plaintiff and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by AT&T as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiff be granted the declaratory relief sought herein;

7. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre-judgment and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

DATED this 12th day of August, 2024.

KELLER ROHRBACK L.L.P.

By: */s/ Christopher L. Springer*

Christopher L. Springer (SBN 291180)
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Telephone: (805) 456-1496
Facsimile: (805) 456-1497
cspringer@kellerrohrback.com

Benjamin Gould (SBN 250630)
Cari Campen Laufenberg (*pro hac vice* to follow)
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
Telephone: (206) 623-1900
Facsimile: (206) 623-3384
bgould@kellerrohrback.com
claufenberg@kellerrohrback.com

Matthew S. Melamed (SBN 260272)
180 Grand Avenue, Suite 1380
Oakland, CA 94612
Telephone: (510) 463-3900
Facsimile: (510) 463-3901
mmelamed@kellerrohrback.com

Attorneys for Plaintiff Ghanaat